MESSAGE M	CRC(M)	PADDING
n bits	p bits	q bits

FIG.1 (Prior Art)

MESSAGE M	SEAL	CRC	PADDING
n bits	p1bits	p2bits	1 1
	p bits		

FIG.2

MESSAGE M	SEAL	PADDING
n bits	p1=pbits	q bits

F 16.3